Department of Homeland Security Daily Open Source Infrastructure Report for 09 December 2005

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Immigration and Customs Enforcement reports a Bellevue, Washington man pleaded guilty in U.S. District Court in Seattle on Tuesday, December 6, to charges that he illegally exported night vision goggles and camera lenses to Taiwan; this equipment was ultimately shipped to the People's Republic of China. (See item 3)
- WABC reports an Egyptian man whose sneakers tested positive for explosives at New York's John F. Kennedy International Airport, was detained by Transportation Security Administration officials, but then allowed to board another flight while his shoes were sent to a lab for further examination. (See item 11)
- The Boston Globe reports Boston's Mayor Thomas M. Menino has detailed an $827,500 emergency preparedness plan that could evacuate Boston within hours, notifying residents by automated phone calls, directing traffic to evacuation routes, and putting residents without cars on buses and other city vehicles. (See item 25)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1.

December 08, Associated Press — **Gas plant explodes.** An explosion at a West Texas gas plant near Crane on Wednesday, December 7, could be seen as far as 20 miles away and shook homes in Odessa. There were no injuries or deaths in the explosion at the compressor station in Crane County. Darrell Johnston, acting battalion chief of the Odessa fire department, said the fire apparently started in three massive holding tanks, which contained about 10,000 gallons each of drip gasoline, which is an untreated, unrefined gasoline directly from the ground. "There was some liquid runoff that caught a cooling tower on fire," Crane Fire Chief Gary Collier said. "And there were some associate fires caused by the explosion that were pretty easy to put out," said Collier. Johnston said that the explosion also blew shrapnel into the air.
Source: http://abclocal.go.com/ktrk/story?section=state&id=3705994

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *December 08, San Diego Union−Tribune (CA)* — **Fuel tanker catches fire near stadium in California.** A fuel tanker overturned and caught fire near the main entrance to Qualcomm Stadium Wednesday morning, December 7, sending black smoke over Mission Valley, CA, and spilling fuel into storm drains that feed the San Diego River. The fire burned itself out shortly after 11 a.m. PST. Several roads in the area were closed into the afternoon. No injuries were reported and there were no evacuations. The tank that overturned was one of two being towed by a tanker truck. Firefighters said the first tank was empty, while the second contained an estimated 4,000 gallons of gasoline. Jeff Bowman, chief of the San Diego Fire−Rescue Department, said the uneven load contributed to the crash as the driver was making a turn after leaving a fuel tank farm across Friars Road. Deputy City Manager Larry Gardner said the city's main concern was to get control of the storm drains, water and sewer systems and to try to prevent further contamination from gasoline and runoff. At least one explosion was reported in an underground storm drain where gas fumes ignited, said San Diego Fire−Rescue Department spokesperson Maurice Luque.
Source: http://www.signonsandiego.com//uniontrib/20051208/news_7m8ta nker.html

[Return to top]

Defense Industrial Base Sector

3. *December 06, Immigration and Customs Enforcement* — **Man pleads guilty to violating arms export act.** A Bellevue, WA, man pleaded guilty in U.S. District Court in Seattle on Tuesday, December 6, to charges that he illegally exported night vision goggles and camera lenses to Taiwan. The military equipment was ultimately shipped to the People's Republic of China. Howard Hsy was charged with violating the terms of the Arms Export Control Act. The equipment in question is primarily used by military pilots to fly and navigate at night. Exporting these items requires a license and written approval from the U.S. State Department, which Hsy did not have. Documents filed in the case reveal that Hsy was approached by an unnamed co−conspirator in Taiwan who asked Hsy to acquire the following military items: Imaging Systems F4949 "Generation III" night−vision goggles; HGV 55/P Helmet Mount Assemblies; and Nightmate CCTV Adapter "Generation III" night−vision camera lenses. Hsy,

Donald Shull, and a third Seattle area co−conspirator purchased the items through a front company they had in Auburn, WA. Over the course of about 18 months, the items were purchased and delivered to the co−conspirator in Taiwan, who shipped the military items to China.
Source: http://www.ice.gov/graphics/news/newsreleases/articles/05120 6seattle.htm

[Return to top]

Banking and Finance Sector

4. *December 08, Associated Press* — **Community college posted personal information, warns students.** More than 26,000 community college students whose personal information was posted on the Internet for months are being warned to guard against identity theft. The personal information −− names, Social Security numbers and addresses −− was from students who took noncredit classes at J. Sargeant Reynolds Community College from 2000 to 2003. The information was compiled for a mailing list and posted on the college's Web server by an employee, said Malcolm Holmes, the college's director of marketing and public relations. A student made the discovery after he found the information through a search engine. Holmes said the college immediately contacted Google and believed the company was removing copies of the information from its servers, however, officials realized the information was still available in cyberspace when a second student contacted the school late last month. College officials again contacted Google, Holmes said. "We've gotten no reports of identity theft or anybody doing anything with their personal information," he added.
Source: http://www.dailypress.com/news/local/virginia/dp−va−−college −identityt1208dec08,0,630332.story?coll=dp−headlines−virgini a

5. *December 07, Reuters* — **Fears over identity theft exaggerated, study suggests.** A new study suggests consumers whose credit cards are lost or stolen or whose personal information is accidentally compromised face little risk of becoming victims of identity theft. The analysis, released on Wednesday, December 7, also found that even in the most dangerous data breaches −− where thieves access social security numbers and other sensitive information on consumers they have deliberately targeted −− only about one in 1,000 victims had their identities stolen. ID Analytics, the San Diego, CA−based fraud detection company that performed the analysis, said it looked at four recent data breaches involving a total of 500,000 consumers. It declined to provide the names of the companies involved in the breaches, but Mike Cook, ID Analytics co−founder, said one of them was a top five U.S. bank. After six months of study, comparing compromised information against credit applications, ID Analytics said it discovered that the smaller the breach, the greater the likelihood the information was subsequently used by scammers to hijack the identity of victims. “If you’re in a breach of 100, 200 or 250 names, there’s a pretty high probability that you’re identity is going to be used,” said Cook.
National Data Breach Analysis:
http://www.idanalytics.com/pdf/Breach_Analysis_Overview.pdf
Source: http://msnbc.msn.com/id/10372317/

6. *December 07, Wood−TV (MI)* — **Identity theft ring suspects may be part of larger organization.** Stanislav Botiyenko and Vladimir Zhdanovich were charged Wednesday, December 7, after police say they allegedly stole identities and then merchandise. The men

were charged with three felony counts each, including possessing and using stolen credit cards, using a computer to commit an illegal act, and racketeering; in this case, conducting an illegal enterprise using stolen credit cards. "This is clearly an organized crime unit that is very sophisticated," said Muskegon, MI, County Prosecutor Tony Tague. It is an elaborate plot using those stolen credit cards to order electronics over the Internet. "They were able to duplicate credit cards to such an extent that they were able to get around security at stores which have special security devices installed," adds Tague. Authorities believe the two men are part of a sophisticated Russian organized crime ring after discovering high−tech items and cell phones in their van. The high−tech devices are capable of altering magnetic strips on credit cards. The investigation is now spreading to other sites after authorities traced stolen credit cards "including Illinois, Indiana, Arizona, Colorado," Tague says.
Source: http://www.msnbc.msn.com/id/10371988/

7. *December 07, IDG News Service* — **New York breach notification law goes into effect.** New York has joined the growing list of states requiring that companies notify their customers whenever private information has been compromised. The state's Information Security Breach and Notification Act went into effect Wednesday, December 7, according to a spokesperson for the state's attorney general, Eliot Spitzer. The law, which is similar to California's SB−1386 notification law, requires businesses and state agencies to inform New York residents "whose unencrpyted personal information may have been acquired by an unauthorized person," according to the text of the legislation.
Source: http://www.computerworld.com/governmenttopics/government/legislation/story/0,10801,106850,00.html

[Return to top]

Transportation and Border Security Sector

8. *December 08, Associated Press* — **Southwest Airlines pilots to fly more hours.** Pilots at Southwest Airlines will be flying one and a half more hours each month after the pilot's union and the Dallas−based carrier struck an agreement. That would save Southwest about $4 million annually, because the discounter won't need to hire as many pilots as it expands its schedule about 10 percent a year, the Southwest Airlines Pilots' Association said. The airline's 4,700 pilots had about 67 hours of actual flying time a month before the latest agreement, reached November 6, goes into effect. Southwest pilots used to average about 70 hours a month a decade ago, the carrier's union officials say. But as the pilots have gained seniority, they've also earned more vacation. After Southwest asked the union for the extra productivity, the two sides came to terms in a side letter separate from their current contract.
Source: http://www.usatoday.com/travel/news/2005−12−08−swa−pilots_x. htm

9. *December 08, Associated Press* — **Firearm seizures up at New Orleans airport.** When an airport security officer saw an image of a gun on an X−ray machine at a passenger concourse, he immediately hit the test button to determine if the weapon was real or a fictional setup designed to keep screeners on their toes. Unlike most instances, the image didn't vanish from the screen, indicating to officer Kevin Forest the threat was real. The situation was one of 10 at New Orleans' Louis Armstrong International since October, said Mike Robinson, the airport's security director. The airport has had 17 such seizures in the last year, so 10 in two months is

significant, he said. Robinson said weapons seizures are up at airports around the country, but because passenger volume is not yet at pre−Katrina levels, the sudden jump puts the New Orleans airport way above the national average. Robinson said most of the incidents involved local residents. Those involved ranged from a local attorney to an individual wanted on three felony charges. The latter was arrested on site, Robinson said. If a passenger has no previous record, some penalties may be deferred, but fines can be as high as $7,500, Robinson said.
Source: http://www.usatoday.com/travel/news/2005−12−08−no−airport−gu ns_x.htm

10. *December 08, Washington Times* — **Agents pledged to guard Southwest border.** Department of Homeland Security Secretary Michael Chertoff said on Wednesday, December 7, that 1,700 new U.S. Border Patrol agents will be assigned next year for what he called a "key element" in the government's ongoing effort to secure the Southwest border. Last year, Border Patrol agents apprehended 1.15 million foreigners trying to sneak in between U.S. land ports of entry −− more than 3,100 a day −− a 24 percent increase from the year before. About half of them were caught trying to cross through Arizona. Border Patrol Chief David V. Aguilar said the additional agent staffing −− which will be assigned between the ports of entry −− would "have immediate impact in securing our country from the threat of terrorism while improving the quality of life of communities along the border." The new agents are part of a multiyear plan to secure U.S. borders and reduce illegal immigration. Known as the Secure Border Initiative, it is designed to enable the department to gain operational control of the northern and southern borders within five years.
Secure Border Initiative Update: http://www.dhs.gov/dhspublic/display?content=5024
Source: http://washingtontimes.com/national/20051208−121139−2217r.ht m

11. *December 08, WABC (NY)* — **Questions surround alleged New York's John F. Kennedy International Airport shoe bomb incident.** There are serious security questions at New York's John F. Kennedy International Airport after an Egyptian man was stopped Friday, December 2, because preliminary tests showed his shoes contained an explosive material. Law enforcement sources are calling it a major breakdown in protocol. An Egyptian man whose sneakers tested positive for explosives, was detained by Transportation Security Administration (TSA) officials, but allowed to board another flight while his shoes were sent to a lab for further examination. According to an internal document obtained by WABC Eyewitness News, TSA maintained custody of the shoes and released the passenger as per the direction of the TSA operations manager. The man, who claimed to be a student at the University of Iowa, was re−booked on another flight. A spokesman for the university told Eyewitness News they have no record of him being enrolled there. The FBI says the incident created an atmosphere of tension, which prompted an alert of a potential shoe bomber on the loose.
FBI release: http://www.fbi.gov/pressrel/pressrel05/egytiandetention12080 5.htm
Source: http://abclocal.go.com/wabc/story?section=local&id=3708084

[Return to top]

Postal and Shipping Sector

12. *December 07, Today* — **U.S. Postal Service wants contract carriers to be exempted from new hours−of−service rules.** The U.S. Postal Service (USPS) is asking the Department of Transportation to exempt its contracted motor carriers from the new hours−of−service (HOS)

rules. USPS has submitted an application to the Federal Motor Carrier Safety Administration to allow an unspecified number of carriers that transport for USPS to revert back to the HOS rules in place before January 2004. USPS, as an independent agency of the executive branch of the U.S. government, is exempted. However, the regulation states any motor carrier under contract with such firms remains subject to the HOS rules. If granted, the exemption would have a serious affect on private parcel delivery companies, which, by complying with a more stringent HOS regime, may be placed at a competitive disadvantage. USPS argues the exemption "would achieve a level of safety equivalent to, or greater than, the level of safety obtained under the current 14−hour rule..."
Source: http://www.todaystrucking.com/news.cfm?intDocID=14167

13. *December 01, Mobile Register (AL)* — **Cleaner accused of stealing money orders at post office.** Money orders at the downtown Mobile, AL, post office apparently proved too tempting for a woman hired to clean out the building following Hurricane Katrina, according a federal indictment charging her with embezzlement. Investigators from the U.S. Postal Inspection Service contend that Sofia Nicole Cross, 21, of Mobile took seven money orders. Mike Willis, the team leader for postal investigators, said Cross was a temporary worker hired by a contractor that was performing work at the building at Royal and Congress streets. Cross allegedly took the money orders, for amounts ranging from $110 to $310, and made them out to herself and others she knew. Assistant U.S. Attorney Daryl Atchison said the checks, totaling $1,525, were cashed at various locations between Saturday, September 3 and Monday, September 12.
Source: http://www.al.com/news/mobileregister/index.ssf?/base/news/1133432130291290.xml&coll=3

14. *December 01, The Journal News (NY)* — **Two armed men rob New York post office.** Two masked men robbed the Valhalla, NY, post office at gunpoint early on Wednesday, November 30, making off with an undetermined number of stamps after leaving a lone postal employee handcuffed to a bathroom sink. "The employee was not physically injured," U.S. Postal Inspector Al Weissmann said. The robbery occurred about 4:30 a.m. EST at the post office at 10 Cleveland Street. Weissmann said two men wearing dark ski masks and dark clothing apparently entered through the back of the building, surprised the postal worker, and forced him to take them to a back office where the safe is located. Weissmann said, "They managed to take rolls of stamps...We don't know the value yet −− we're still counting −− but we don't believe that it was a substantial amount." He said the postal employee was forced into a bathroom, where he was left handcuffed to a sink. It was unclear exactly how the robbers entered or left the post office. Police notified the Postal Inspection Service, which sent members of its major crimes team to take control of the investigation.
Source: http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/20051201/NEWS02/512010374/1018

[Return to top]

Agriculture Sector

15. *December 07, Stop Soybean Rust News* — **Soybean rust found on kudzu in Louisiana.** The U.S. Department of Agriculture has confirmed the first soybean rust find on kudzu in

Louisiana, in Tangipahoa Parish. This is the second incidence of soybean rust in the state this year, and the 137th positive county/parish in the U.S. A kudzu sample collected on November 18 in Amite, Tangipahoa Parish, tested positive for Asian soybean rust. Amite is north of Lake Pontchartrain, about 40 miles east of Baton Rouge. The first soybean rust of 2005 found in Louisiana was discovered on soybean on October 28 in East Baton Rouge Parish, two parishes west of Tangipahoa Parish.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=652

16. *December 07, Ohio Ag Connection* — **More emerald ash borer discovered Ohio.** Ohio Department of Agriculture officials Tuesday, December 6, announced the discovery of Emerald ash borer (EAB), a destructive exotic insect from Asia, in ash trees in western Lorain County. The discovery, near the county border, is connected to a series of recent finds in eastern Erie County. Department surveyors have begun work to determine the extent of the infestation. Department officials discovered a succession of infested trees while examining ash trees at mile markers along Interstate Highway 80/90. "Finding Emerald Ash Borer along the turnpike is a reminder that citizens must be diligent in abiding by the quarantines and not moving firewood," said Ohio Agriculture Director Fred Dailey. "As the colder months set in and firewood sales pick up, Ohioans should be cognizant that it only takes one piece of infested firewood to kill millions of ash trees." At this time, the origin of infestation is unknown, but it likely started as a result of the transportation of firewood, ash tree nursery stock, ash logs, or other ash tree materials from a quarantined area. Department surveyors will work to determine the origin of infestation in Lorain County's Henrietta Township and Erie County's Florence Township.
EAB information: http://www.emeraldashborer.info/
Source: http://www.ohioagconnection.com/story−state.cfm?Id=587&yr=20 05

[Return to top]

Food Sector

17. *December 08, Reuters* — **Japan panel approves restart of U.S. beef imports.** Japan's Food Safety Commission said on Thursday, December 8, it had approved the easing of a two−year government ban on U.S. and Canadian beef imposed due to mad cow disease, paving the way for partial imports to resume this month. Finalizing a report compiled in October by its subcommittee, the commission concluded that beef and beef offal from North American cattle aged up to 20 months were at very low risk from the brain−wasting disease if risk materials were removed. The Japanese government has said it would swiftly open the border to beef from such young American cattle if the commission gave formal approval, while keeping a ban on beef from older cattle. Japanese media reported this week that the government Monday, December 12, would officially announce an easing of the ban. Japan banned U.S. beef and beef products in December 2003 after the discovery of the first U.S. case of mad cow disease, officially known as bovine spongiform encephalopathy, in Washington state. Before the ban, Japan was the top importer of U.S. beef, with imports valued at $1.4 billion in 2003. Japan banned imports of Canadian beef and beef products in May 2003 after the first Canadian case of BSE was confirmed.
Source: http://www.boston.com/news/world/asia/articles/2005/12/08/japan_panel_approves_restart_of_us_beef_imports_1134054332/

[Return to top]

Water Sector

18. *December 09, Caspar Star Tribune (WY)* — **Oil spill persists in Wyoming.** Illegal oil dumping continued at a commercial wastewater disposal facility in Linch, WY for at least four months despite ongoing monitoring of the situation by the Wyoming Department of Environmental Quality (DEQ). Although the pollution is not an imminent threat to human health, according to John Wagner, director of DEQ's Water Quality Division, the violations remain unresolved, and nothing prevents Sierra Construction Co. and Linch Environmental Contractors Inc. from continuing to use the facilities. Agency field inspectors first made contact with Sierra Construction Co. and Linch Environmental Contractors Inc. in July after discovering a water treatment pond leaking petroleum wastewater to a highway barrow ditch which led to a natural drainage. They also discovered that petroleum wastewater had been illegally dumped in at least one nearby scoria pit. One scoria pit was later excavated and the contaminated material was allegedly spread on a gravel road without a proper permit, according to DEQ documents. Field inspections indicated the pollution continued as recently as Thursday, Novemer 10.
Source: http://www.jacksonholestartrib.com/articles/2005/12/06/news/wyoming/2012527b167afc9f872570cf00008849.txt

[Return to top]

Public Health Sector

19. *December 08, Associated Press* — **China reports fifth human case of bird flu.** A poultry worker in northeast China has tested positive for the H5N1 strain of bird flu, the government said Thursday, December 8, making her the country's fifth confirmed human case of the disease. The 31−year−old woman, surnamed Liu, was sickened October 30 in Heishan County in Liaoning province. She was released from the hospital November 29.
Source: http://www.cbsnews.com/stories/2005/12/08/ap/health/mainD8EC 3AU02.shtml

20. *December 07, Agence France−Presse* — **Vietnam bans Tamiflu sales to build up stockpile.** Vietnam has banned over−the−counter sales of bird flu drug Tamiflu to build up a national stockpile in case of a mass outbreak. Health Minister Tran Thi Trung Chien gave the order early last month in the face of intense demand for the drug, which does not cure the disease but reduces its impact. A circular was issued on November 23 to provide details, said Cao Minh Quang, director of the ministry's pharmaceutical administration department. Provincial health services have been asked "not to sell Tamiflu doses locally and to stockpile them in national reserves, so that they could be used in areas contaminated by bird flu and in those where there are risks of contamination to humans", Quang said. Swiss manufacturer Roche has agreed to supply Vietnam with 25 million Tamiflu capsules before the end of 2006. The company is also in talks with eight companies to produce the drug locally. Vietnam is the country hit hardest by bird flu. Since late 2003, as many as 93 people have taken ill with the virus and 42 of them have died, according to government figures.
Source: http://news.yahoo.com/s/afp/20051207/hl_afp/healthfluvietnam

tamiflu_051207120527;_ylt=Amf3vu4o10w0vMDoKzK3582JOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

21. *December 07, Associated Press* — **White House to hold flu response exercise.** The White House is hosting a top−level exercise this weekend to test the federal government's plans for responding to any flu pandemic outbreak in the U.S. The four−hour "tabletop exercise" is being held Saturday, December 10, at the White House and will be attended by Cabinet secretaries and other top government officials, but not the president, White House press secretary Scott McClellan said Wednesday, December 7. "We have done much to plan for a pandemic," McClellan said. "But planning alone is not enough. Plans must be tested and improved upon." McClellan did not give other details of how the exercise would be conducted.
Source: http://www.cbsnews.com/stories/2005/12/07/ap/health/mainD8EB H2OGC.shtml

22. *November 11, Clinical Infectious Diseases* — **Clinical characteristics of human monkeypox, and risk factors for severe disease.** Human monkeypox is an emerging smallpox−like illness that was identified for the first time in the U.S. during an outbreak in 2003. Knowledge of the clinical manifestations of monkeypox in adults is limited, and clinical laboratory findings have been unknown. Demographic information; medical history; smallpox vaccination status; signs, symptoms, and duration of illness, and laboratory results were extracted from medical records of patients with a confirmed case of monkeypox in the U.S. Two−way comparisons were conducted between pediatric and adult patients and between patients with and patients without previous smallpox vaccination. Bivariate and multivariate analyses of risk factors for severe disease (temperature greater than 38.3°C) and the presence of rash (100 lesions), activity and duration of hospitalization, and abnormal clinical laboratory findings were performed. Of 34 patients five (15 percent) were defined as severely ill, and nine (26 percent) were hospitalized for more than 48 hours. Previous smallpox vaccination was not associated with disease severity or hospitalization. Pediatric patients were more likely to be hospitalized in an intensive care unit. Vomiting and mouth sores were independently associated with a hospitalization duration of more than 48 hours and with having three laboratory tests with abnormal results.
Source: http://www.journals.uchicago.edu/CID/journal/issues/v41n12/3 6967/36967.html

[Return to top]

Government Sector

23. *December 07, Department of Homeland Security* — **DHS and NASA sign technology agreement.** Department of Homeland Security (DHS) Under Secretary for Science and Technology Dr. Charles McQueary joined National Aeronautics and Space Administration's (NASA) Assistant Administrator David Saleeba in signing a Memorandum of Understanding on Wednesday, December 7, to collaborate and coordinate on appropriate research and development projects. The agreement allows DHS Science and Technology directorate and NASA to share expertise and technologies to the benefit of both agencies and the public they serve. The Memorandum of Understanding provides a mechanism for DHS and NASA to coordinate on the evaluation of existing technologies, acceleration of promising technologies, undertaking joint research and development, sharing resources and personnel, and working with the private sector and other public agencies in joint programs. The agencies will share information, leverage U.S. government resources and assets, and promote best practices.

Source: http://www.dhs.gov/dhspublic/display?content=5021

[Return to top]

Emergency Services Sector

24. *December 07, Fleet Owner* — **Highway Watch to share intelligence directly with Emergency Management and Response network.** The Highway Watch program will begin disseminating reports from its Information Sharing and Analysis Center (ISAC) directly to the Emergency Management and Response's (EMR) ISAC network. Prior to this, the EMR received Highway Watch data through the U.S. Department of Homeland Security and other sources. "This new alliance automatically puts the Highway Watch information into the hands of first responders in every major city in the country," said Don L. Rondeau, director of the Highway ISAC. "It greatly enhances our ability to immediately mobilize and respond to an incident and that increased capacity to react will pay tremendous dividends in our efforts to keep America safe and secure." The EMR−ISAC network is comprised of 22,000 first responders including fire departments, law enforcement personnel, emergency medical technicians, and state emergency management personnel.
Highway Watch program: http://www.highwaywatch.com/
Source: http://fleetowner.com/news/highway_watch_share_emr_120705/

25. *December 07, Boston Globe (MA)* — **Massachusetts mayor details emergency evacuation plan.** Boston's Mayor Thomas M. Menino detailed an $827,500 emergency preparedness plan Wednesday, December 7, that could evacuate Boston within hours, notifying residents by automated phone calls, directing traffic to evacuation routes marked with 400 new blue−and−white signs, and putting residents without cars on buses and other city vehicles. The blueprint is meant to be adaptable to "all hazards," Menino said. The hazards include natural disasters, infrastructure failures, and manmade disasters such as fires or terrorist attacks. Boston police would coordinate any evacuation, drawing on all available personnel from other city and state agencies. Under the new Mayor's Emergency Alert Notification System, or MEANS, the city would notify all residents by phone within a few hours. The system, to take effect in January, can automatically telephone up to 60,000 residents an hour, leaving an automated message. Officials also began mailing a brochure detailing the evacuation plan to all of the city's 280,000 households. The brochure has been translated into Spanish and includes a map of the evacuation routes. A new city website, www.cityofboston.gov/emergency, will offer the same information translated into six languages, Menino said. The plan does not include any shelters where thousands of people could flee in an emergency.
City of Boston Emergency Preparedness Website: http://www.cityofboston.gov/emergency/
Source: http://www.boston.com/news/local/massachusetts/articles/2005/12/07/menino_details_emergency_evacuation_plan/

[Return to top]

Information Technology and Telecommunications Sector

26.

December 08, VNU Net — **Rootkits storm malware chart.** The most common rootkit is a spyware application known as Apropos, according to data collected by security experts at F−Secure. Apropos collects system information and data on a user's browsing habits and sends the information back to the application's creators. It is also capable of recording keystrokes and launching a denial of service attack, and can download and install additional software on an infected computer. Rootkits have become a mainstream phenomenon ever since Sony BMG was caught bundling one as part of the XCP anti−piracy technology on some of its audio CDs. Sony used a rootkit to hide the technology, preventing users from uninstalling the application. Hackers originally started using rootkits to build backdoors into computers, but the technology has caught a second wind in recent months as malware creators use rootkits to hide worms and spyware from antivirus and anti−spyware software. In F−Secure's ranking Apropos surpassed the Sony BMG rootkit in the number of infections.
Source: http://www.vnunet.com/vnunet/news/2147301/rootkits−storm−mal ware−chart

27. *December 07, TechWeb News* — **Next Sober attack slated for January 5.** The next big Sober worm attack is scheduled to take place Thursday, January 5, 2006, a date probably picked because it's the 87th anniversary of the founding of a precursor to the Nazi Party, a security firm said Wednesday, December 7. January 5, 2006, was the date embedded in the most recent Sober variants, said Ken Dunham, a senior engineer with Reston, VA−based VeriSign iDefense, a security intelligence firm. "We did reverse engineering on the variants, and found this date in the code," said Dunham. "The way this works is that at a pre−determined time, computers already infected with Sober will connect with specified servers and download a new payload, which will likely be spammed out in the millions, as was the last version." Sober, which boasts more than 30 variants, debuted more than two years ago, and is characterized by bilingual messages (English or German) that are mass−mailed in huge quantities. The worm's creator doesn't appear to be motivated by money. Instead, the creator −− who is assumed to be German −− has a political agenda, said Ramses Martinez, iDefense's director of malicious code operations. "There hasn't been one variant that did anything but send out right−wing German spam."
Source: http://www.techweb.com/wire/security/174904530

28. *December 07, Associated Press* — **Federal Bureau of Investigation: Terror groups lack ability to mount crippling Internet−based attacks.** Al Qaeda and other terror groups are more sophisticated in their use of computers but still are unable to mount crippling Internet−based attacks against U.S. power grids, airports and other targets, the Federal Bureau of Investigation's (FBI) top cyber crime official said Wednesday, December 7. Investigators keep a close watch on terror groups' use of computers but have not detected any plans to launch cyber attacks against major public institutions in the United States, FBI assistant director Louis M. Reigel said. The government has conducted simulated terrorist attacks on computer, banking, and utility systems, and Reigel said his division of around 1,100 agents treats seriously the prospect of such a strike. FBI cyber experts have noticed progress in the technical mastery suspected terrorists have shown online, he said. Terrorists also have made only infrequent use of stenography, the practice of hiding a text message in another kind of file, typically a picture, Reigel said.
Source: http://abcnews.go.com/Politics/wireStory?id=1383901

29.

December 07, Federal Computer Weekly — **Companies form IPv6 test center.** Spirent Federal Systems and v6 Transition are establishing an IPv6 test center in Northern Virginia. It will allow federal agencies to test networks and products for IPv6 capability in preparation for meeting a June 2008 deadline for adopting the technology. The Office of Management and Budget imposed the deadline for agencies to upgrade from the current IPv4 to IPv6. When completed, the test center will provide customers with the latest testing equipment and the support of security−cleared engineers. The companies did not reveal a planned opening date. IPv6 offers many advantages over IPv4, including vastly expanded address space to allow more unique IP addresses, along with tighter security and more efficient network management capabilities.
Source: http://www.fcw.com/article91642−12−07−05−Web

30. *December 07, VNU Net* — **Microsoft and eBay hook up to catch pirated software.** Microsoft and eBay are working together to stop the sale of pirated software on the online auction site. The companies said in a statement that over 21,000 suspect software sales were removed from the eBay United Kingdom site between August and October this year. Around half were sales of counterfeit copies of Windows, and 36 percent were fake copies of Microsoft Office. Microsoft claimed that the crackdown is working because eBay removed 11,535 suspected counterfeit sales from the site in August. This fell to 4,460 in September and 5,423 in October.
Source: http://www.vnunet.com/vnunet/news/2147277/ebay−tackles−micro soft−software

31. *December 06, TechWeb News* — **Security threats increase in 2005.** The number of new worms, viruses, and Trojan horses jumped 48 percent in 2005, a security company said Tuesday, December 6, as it detailed the year's security woes. United Kingdom−based Sophos detected nearly 16,000 new threats from January to November, 2005, a major bump from the 10,724 during the same period in 2004. Every month in 2005 posted larger−than−last−year numbers, but November, which was marked by the debut of a strong Sober.z worm, outpaced all others. By Sophos' records, 1,940 new viruses, worms, Trojans, and spyware threats were spotted last month, its largest−ever monthly increase. If that pace were to continue, the next 12 months would see 23,000 threats. Topping Sophos' top−10 chart was the long−running Zafi.d, a mass−mailed worm that made itself known almost a year ago: It accounted for 16.7 percent of all threats detected during the first 11 months of 2005. Netsky.p took second place, with 15.7 percent, while the new Sober.z came in at third, with six percent. "Given more time, Sober.z would have dominated the chart, but its emergence in late November prevented it from taking pole position," said Graham Cluley, senior technology consultant at Sophos.
Source: http://www.techweb.com/wire/security/174901293

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of functionality that

could allow the mass mailing worm known as "W32/Sober.X" to automatically update itself. W32/Sober.X is a bi−lingual (English and German) mass mailing worm that utilizes its own SMTP engine to propagate. The W32/Sober.X worm began propagating on November 15, 2005 and will attempt to update itself on or around January 5, 2006. Systems that have already been compromised by the W32/Sober.X worm are expected to receive this update. Once the update is received, the W32/Sober.X worm may execute code that reduces the security protection of vulnerable systems. US−CERT strongly recommends that users and administrators implement the following general protection measures:

Install anti−virus software, and keep its virus signature files up to date.

Do not follow unsolicited Web links or execute attachments received in email messages, even if sent by a known and trusted source.

Keep up to date on patches and fixes for your operating system.

For more information please review the US−CERT Computer Virus Resources at URL: http://www.us−cert.gov/other_sources/viruses.html

Reports of IRS Phishing Emails: US−CERT has received reports of a phishing email scam that attempts to convince the user that it is from the Internal Revenue Service (IRS) by using a spoofed "From" address of "tax−refunds@irs.gov".

For additional information on ways to avoid phishing email attacks, US−CERT recommends that all users review the following:
Avoiding Social Engineering and Phishing Attacks at URL:
http://www.us−cert.gov/cas/tips/ST04−014.html

Spoofed/Forged Email at URL: http://www.cert.org/tech_tips/email_spoofing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 4142 (oidocsvc), 80 (www), 6346 (gnutella−svc), 50497 (−−−), 55556 (−−−), 139 (netbios−ssn), 135 (epmap) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer